UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,925	06/24/2003	Basil Treppa	104393.00031	4336

32294 7590 06/22/2009

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
HIGA, BRENDAN Y	

ART UNIT	PAPER NUMBER
2453	

MAIL DATE	DELIVERY MODE
06/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/603,925	TREPPA ET AL.	
	Examiner	Art Unit	
	BRENDAN Y. HIGA	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-20,22-25 and 27-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-20,22-25 and 27-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on April 08, 2009 has been entered.

Claims 1-9, 11-20, 22-25 and 27-34 are pending.

Claim Objections

Claim 14 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 9, 16, 18, 19, 24, 25, 30 and 31 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 1, 9, 18, 24, 30 and 31 the limitation "*the most recent successful configuration*" lacks antecedent basis. For the purpose of this office action, the examiner has interpreted the claim to read "[[the]] a most recent successful configuration".

Regarding claims 16 and 19, as per the limitation *"applying a configuration lock to prevent other application from performing network management operations on the devices within the cluster"*, it is unclear if this is a new or second configuration lock separate from the configuration lock of claims 9 and 18, respectively.
For the purpose of this office action the examiner has interpreted the claim to read:
"...~~applying a configuration lock to prevent other applications from performing network management operations on the devices within the cluster~~ applying said configuration lock during a predetermined time; and releasing the configuration lock after the network management operations are performed".
Similarly with respect to claim 19, the examiner has interpreted the claim to read:
"...~~applying a configuration lock to prevent other applications from performing network management operations on the devices within the cluster~~ applying said configuration lock during a predetermined time."

Regarding claims 25, as per the limitation *"third applying means for applying a configuration lock to prevent other applications from performing network management operations on the devices within the cluster"*, the specification does not appear to

disclose a third applying means that is separate from the first applying means for applying a configuration lock to prevent other applications from performing network management operations on the at least two devices within the cluster. For the purpose of this office action the examiner has interpreted claim 25 to read:

"...~~third applying means for applying a configuration lock to prevent other applications from performing network management operations on the devices within the cluster~~ said first applying means applying said configuration lock during a predetermined time"

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6, 9, 11-14, 16-19, 20, 23-25, and 30-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slaughter et al. (US 6,014,669) ("Slaughter") in view of John et al. (US 7,403,993)("John").

As per claim 1, Slaughter teaches a system, comprising:

a network interface configured to communicate with nodes in a cluster (see col. 6, lines 1-3, wherein the step of issuing an update request to cluster server 106B, implies a network interface);

a configuration subsystem (see "client" Fig. 2, 108A-D) operationally coupled to a remote management broker (see "master server", col. 6, lines 15-67), wherein the remote management broker is configured to distribute information between the nodes in the cluster (see col. 6, lines 34-36, "broadcasting an update request"); and

a processor (see col. 1, lines 16-17) configured to

access the cluster from a single-point (see abstract, *"configuration database operations can be performed from any node"*, read as accessing the cluster from any single point in the cluster),

determine network management operations to perform on the cluster (see col. 6, lines 1-3, wherein the issuance of an update request implies a determination that an update operation is to be performed on the cluster),

apply a configuration lock to prevent other applications from performing network management operations on the at least two devices within the cluster (i.e. "global locking mechanism", see abstract and col. 6, lines 15-34)

perform the determined network management operations (i.e. apply updated configuration information, see col. 6, lines 31-45), and

determine whether the network management operations on the cluster, including said at least two devices, were applied correctly (see col. 5, lines 34-42), and

when the network management operations were not applied correctly, the

processor is configured to roll back to the most recent successful configuration (see col. 5, lines 34-42 and col. 6, lines 41-60, *wherein a shadow copy representing the previous state (read as a most recent successful configuration) is restored in case of an update failure on one of the nodes*).

As per claim 1 Slaughter does not necessarily teach obtaining information relating to at least two devices within the cluster and present the information to a user.

Nevertheless, in the same art of cluster management, John teaches a cluster system including a cluster management console for monitoring and managing a cluster; presenting information to a user; and determining based on user inputs an update to perform on said cluster group (see col. 20, line 38-col. 22, line 65).

A person having ordinary skill in the art would have been motivated to modify the teachings of Slaughter with the teachings of John by communicatively coupling a cluster management console to the communication interface 102, of Slaughter, for monitoring and managing Slaughter's cluster nodes 104-104D. The motivation for doing so would have been to allow an administrator to view or ascertain the operational health of Slaughter's cluster nodes 104-104D (see John, col. 22, lines 15-17).

As per claim 2, Slaughter further teaches wherein the processor is configured to provide a command line interface that is configured to access the cluster (see CCDADM, col. 12, line 40).

As per claim 3, Slaughter does not expressly teach wherein the processor is configured to provide a graphical user interface that is configured to access the cluster. Nevertheless in the same art as noted above, John teaches the use of a graphical user interface that is configured to access the cluster (see "Cluster Management Console", see Fig. 11 and col. 20, line 38-col. 22, line 65).

The same motivation that was utilized for combining Slaughter and John in claim 1 applies equally well to claim 3.

As per claim 4, Slaughter does not expressly teach wherein the process is further configured to aggregate data relating to the devices within the cluster. Nevertheless in the same art as noted above, John teaches the use of a graphical user interface that is configured to aggregate data that is related to devices within a cluster (see "Cluster Management Console", see Fig. 11 and col. 20, line 38-col. 22, line 65, with respect to *"cluster-wide active stream counts"*, see col. 21, lines 65-67, and also *"total number of streams played"*, see col. 22, lines 10-14, read as aggregate data that is related to devices within a cluster).

The same motivation that was utilized for combining Slaughter and John in claim 1 applies equally well to claim 4.

As per claim 6, Slaughter does not expressly teach wherein the remote management broker is further configured to collect attributes from the configuration subsystem. Nevertheless in the same art as noted above, John teaches the need to

configure a system to collect data that is related to devices within a cluster (see "Cluster Management Console", see Fig. 11 and col. 20, line 38-col. 22, line 65, *"the console collects server information, asset information, and load and stream counts…", col. 20, lines 42-45*).

The same motivation that was utilized for combining Slaughter and John in claim 1 applies equally well to claim 6.

As per claim 9, Slaughter teaches a method comprising:

Accessing a cluster from a single-point (see abstract, *"configuration database operations can be performed from any node"*, read as accessing the cluster from any single point in the cluster)

Determining network management operations to perform on the cluster (see col. 6, lines 1-3, wherein the issuance of an update request implies a determination that an update operation is to be performed on the cluster);

Applying a configuration lock to prevent other applications from performing network management operations on the at least two devices within the cluster (i.e. "global locking mechanism", see abstract and col. 6, lines 15-34);

Performing the determined network management operations on the cluster (i.e. apply updated configuration information, see col. 6, lines 31-45); and determining whether the network management operations on the cluster, including said at least two devices, were applied correctly (see col. 5, lines 34-42), and when the network management operations were not applied correctly, rolling back to the most recent

successful configuration (see col. 5, lines 34-42 and col. 6, lines 41-60, *wherein a shadow copy representing the previous state (read as a most recent successful configuration) is restored in case of an update failure on one of the nodes*).

As per claim 9, Slaughter does not expressly teach said method further comprising: obtaining attributes relating to at least two devices within the cluster; presenting the attributes to a user and receiving input from the user relating to the attributes; and determining network management operations to perform on the cluster based on the received input.

Nevertheless, in the same art of cluster management, John teaches a cluster system including a cluster management console for monitoring and managing a cluster; presenting information to a user; and determining based on user inputs an update to perform on said cluster group (see col. 20, line 38-col. 22, line 65).

The same motivation that was utilized for combining Slaughter and John in claim 1 applies equally well to claim 9.

As per claim 11, Slaughter further teaches wherein the processor is configured to provide a command line interface that is configured to access the cluster (see CCDADM, col. 12, line 40).

As per claim 12, Slaughter further teaches distributing information between the nodes in the cluster using a remote management broker determined network

management operations on the cluster further comprises distributing the network management operations to each of the devices (see col. 6, lines 15-67).

As per claim 13, Slaughter further teaches wherein the performing of the determined network management operations on the cluster further comprises distributing the network management operations to each of the devices (see Fig. 2, ref. 102; col. 3, lines 41-45).

As per claim 14, Slaughter further teaches determining whether the network management operations on the cluster were performed correctly, and when the network management operations were not performed correctly, rolling back to a successful configuration (see col. 5, lines 34-42 and col. 6, lines 41-60, *wherein a shadow copy representing the previous state (read as a most recent successful configuration) is restored in case of an update failure on one of the nodes*).

As per claim 16, Slaughter further teaches applying a configuration lock to prevent other applications from performing network management operations on the devices within the cluster during a predetermined time (i.e. "global locking mechanism", see abstract and col. 6, lines 15-34); and

releasing the configuration lock after the network management operations are performed (see col. 6, lines 48-53).

Claims 17, 18, 19, 20, 23, 24, 25, 30, 31, 32, 33 and 34 are rejected under the same rationale as claims 1, 2, 3, 4, 6, 9, 11-14 and 16 since they recite substantially identical subject matter. Any differences between the claims do not result in patentably distinct claims and all of the limitations are taught by the above cited art.

Claims 5, 7, 8, 15, 22 and 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slaughter et al. (US 6,014,669) ("Slaughter") in view of John et al. (US 7,403,993)("John"), in further view of Hickman, Kipp. "The SSL protocol", November 29, 1994 ("Hickman").

As per claim 5, Slaughter further teaches the remote broker further comprises: a remote management broker server (see "master server" Fig. 1, ref. 106A and col. 6, lines 15-67); and a remote management broker client (see client 108B, col. 6, lines 1-14, which initiates a request to the master server 106A).

However, Slaughter does not expressly teach the remote management broker client and the remote management server operationally coupled to a secure transport configured to transport messages;

Nevertheless, a secure transport configured to transport message, such as SSL, was well known in the art, see for example Hickman, Kipp. "The SSL protocol", November 29, 1994.

A person having ordinary skill in the art would have been motivated to modify the teachings of Slaughter with the teachings of "the SSL protocol" by configuring messages - passed between Slaughter's remote management broker server (see "master server" Fig. 1, ref. 106A and col. 6, lines 15-67) and remote management

broker client (see client 108B, col. 6, lines 1-14) - according to a secure transport protocol, such as SSL. The motivation for doing so would have been to enhance security and prevent eavesdropping of messages sent between Slaughter's remote management broker server (see "master server" Fig. 1, ref. 106A and col. 6, lines 15-67) and remote management broker client (see client 108B, col. 6, lines 1-14).

As per claims 7, 15 and 22 Slaughter in view of Hickman further teaches wherein the message include a header to authenticate the messages (see Hickman sec. 1.2 "SSL Record Data Format").

The same motivation that was utilized for combining Slaughter and Hickman in claim 5 applies equally well to claims 7, 15 and 22.

As per claim 8, Slaughter in view of Hickman further teaches wherein the header includes a message authentication code that acts as a shared secret within the cluster (see Hickman "Message Authentication Code", sec. 1.2) and a magic field that identifies one or more of the messages as a remote management broker message (see sec. 1.1, "note that in the long header case (3 bytes total), the second most significant bit in the first byte has special meaning, when zero, the record being sent is a data record", read as a remote management broker [data record] message).

The same motivation that was utilized for combining Slaughter and Hickman in claim 5 applies equally well to claim 8.

As per claim 27-29, Slaughter in view of Hickman further teaches wherein the message authentication code is calculated from contents of the message and from a shared secret value that is known to the devices within the cluster (see Hickman "Message Authentication Code", sec. 1.2, which is computed based on a has of a shared secret value ("secret") and contents of the message ("actual-data").

The same motivation that was utilized for combining Slaughter and Hickman in claim 5 applies equally well to claims 27-29.

Response to Arguments

Applicant's arguments with respect to claims 1-9, 11-20, 22-25 and 27-34 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see PTO 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRENDAN Y. HIGA whose telephone number is (571)272-5823. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571)272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brendan Y Higa/
Examiner, Art Unit 2453

/ARIO ETIENNE/
Supervisory Patent Examiner, Art Unit 2457